Airline passengers'data

Pérez Asinari, María Veroníca; Poullet, Yves

Published in:
Computer Law and Security Report

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

Airline passengers' data: adoption of an adequacy decision by the European Commission. How will the story end?

María Verónica Pérez Asinari & Yves Poullet University of Namur, Belgium

As a consequence of the conflict between US requirements and EU Data Protection legislation, a series of negotiations started

In a recent paper,[1] we have discussed the consequences in EU law of US legislation[2] requiring airline companies to transfer and give access to US authorities to passengers' data. Such consequences have been analyzed *vis-à-vis* the right to privacy and personal data protection from a European point of view. We have also analyzed what would be the proper European legal basis to decide on this issue, and we have studied the documents exchanged between EU and US authorities taking into account the principles that should be respected to reach an "adequate level of protection". This update considers the recent adequacy Decision on the subject from the Commission and other developments in the ongoing discussions across the Atlantic.

A. Introduction

The European Commission has recently adopted an adequacy Decision for the transfer of passenger name record (PNR) data to the US.[3] The application of this instrument is not automatic:

[t]he Decision will enter into force once the US has signed its undertakings and once the international agreement that will complement the adequacy Decision has been signed by the Council and the US.[4]

In this paper we will consider the related developments in this arena in five directions: (1) the new Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP); (2) the actions taken by the European Commission; (3) the reaction by the European Parliament in this regard; (4) a recent Opinion of the Article 29 Personal Data Protection Working Party; and (5) an Opinion of the Belgian Data Protection Authority (DPA) concerning a case submitted to it. We will refer, very briefly, to some of the controversial issues ("*fondo*" and "*forma*") that are still unresolved. It may be that a final word has still to be stated from the European Court of Justice,[5] so this article is simply a follow-up of the recent EU-US dialogue news.

B. Recent developments

As a consequence of the conflict between US requirements and EU Data Protection legislation, a series of negotiations started between both parties in order to reach a solution. A balance between the two different legitimate political interests at stake (the fight against terrorism and the protection to fundamental rights) was required. From a European perspective, the parameters to make a legitimate balance are to be found in Article 8.2 of the European Convention for the Protection of Human Rights and Freedom,[6] the related case-law of the European Court of Human Rights, as well as in Article 13 of the Personal Data Protection Directive.[7]

1. New CBP undertakings

The early Undertakings[8] issued by the CBP authorities have been criticized by the Article 29 Personal Data Protection Working Party[9] for not qualifying for an "adequate level of protection". Moreover, an "Adequacy" decision was not deemed to be sufficient as such to regulate the "transfer" and "access" to personal data, as required by the US legislation. This derived in the consideration of other legal basis[10] to settle that insufficiency.

The new Undertakings[11] are the result of the negotiation process between the European Commission and the CBP, and they address, in principle, the principles of content and enforcement that should be respected for an adequacy declaration.[12]

Basically, the new Undertakings (that consist of 48 points) address the principles as follows:

- **Purpose limitation**: in Point (3), under the title "Use of PNR Data by CBP", it is declared that: "PNR data is issued by CBP strictly for purposes of preventing and combating: 1) terrorism and related crimes; 2) other serious crimes, including organized crime, that are transnational in nature; and 3) flight from warrants or custody for the crimes described above".
- Notwithstanding this clear definition of the purposes it has to be noted that points (34)

Computer Law & Security Report Vol. 20 no. 5 2004 ISSN 0267 3649/04

and (35) of the Undertakings, under the title "Transfer of PNR Data to Other Government Authorities", widen the purposes as follows: (34) "No statement herein shall impede the use or disclosure of PNR data to relevant government authorities, where such disclosure is necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks. Disclosures for these purposes will be subject to the same conditions for transfers set forth in paragraphs 31 and 32 - of these Undertakings"; and (35) "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law.(…)".

- **Data quality and proportionality**: the initial requested 38 PNR items have been reduced to 34 items. In what concerns time limit, there are different periods foreseen. PNR will be kept by CBP during three and a half years. In case the data have been manually accessed, the retention period will be of eight years.
- **Transparency**: Point (36) stated that: "CBP will provide information to the travelling public regarding the PNR requirement and the issues associated with its use (i.e., general information regarding the authority under which the data is collected, the purpose for the collection, protection of the data, data sharing, the identity of the responsible official, procedures available for redress and contact information for persons with questions or concerns, etc., for posting on CBP's website, in travel pamphlets, etc.)".
- **Security**: the measures to be adopted are described in Points (16) to (23) and comprise, among others, the use of a CBP intranet system which is encrypted end-to-end for CBP personnel to have access to PNR; a read-only data base; the fact that no foreign, federal, state or local agency has direct electronic access to PNR data through CBP databases; the fact that only certain CBP officers, employees or information technology contractors have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data; etc.
- **Right of access and rectification**: Point (37) determines: "Requests by the data subject (also known as "first party requesters") to receive a copy of PNR data contained in CBP databases regarding the data subject are processed under the Freedom of Information Act (FOIA). (…)".Then, Point (39) says: "CBP will undertake to rectify data at the request of passengers and crewmembers, air carriers or Data Protection Authorities (DPAs) in the EU Member States (to the extent specifically authorized by the data subject), where CBP determines that such data is contained in its database and a correction is justified and properly supported. CBP will inform any Designated Authority which has received such PNR data of any material rectification of that PNR data".
- **Onward transfers**: Points (28) to (35) declare what would be the policy on "Transfer of PNR Data to Other Government Authorities". Point (29) regulates: "CBP, in its discretion, will only provide PNR data to other government authorities with counter-terrorism or law enforcement functions, on a case-by-case basis, for purposes of preventing and combating offences identified in paragraph 3 herein. (Authorities with whom CBP may share such data shall hereinafter be referred to as the 'Designated Authorities')".
- **Sensitive data**: CBP claims that it "will not use 'sensitive data' (..) from PNR (…)".
- **Enforcement mechanisms**: Point (41) asserts: "In the event that a Data subject's complaint cannot be resolved by CBP, the complaint may be directed, in writing, to the Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, who will review the situation and endeavour to resolve the complaint". Point (42) stipulates: "Additionally, the DHS Privacy Office will address on an expedited basis complaints referred to it by DPAs in the European Union (EU) Member States on behalf of an EU resident to the extent such resident has authorized the DPA to act on his or her behalf and believes that his or her data protection complaint regarding PNR has not been satisfactorily dealt with by CBP (as set out in paragraphs 37-41 of these Undertakings) or the DHS Privacy Office. The Privacy Office will report its conclusions and advise the DPA or DPAs concerned regarding actions taken, if any. The DHS Chief Privacy Officer will include in her report to Congress issues regarding the number, the substance and the resolution of complaints regarding the handling of personal data, such as PNR".

Some other controversial issues have been added to the document:

- **CAPPS II:**[13] the new Undertakings state that CBP may transfer PNRs on a bulk basis to the Transportation Security Administration for "testing" CAPPS II.
- **Reciprocity**: in case the EU decides to adopt an analogue system for passengers' data "CBP would encourage US-based airlines to cooperate".
- **No private right or precedent created**: Point (47) states that "These Undertakings do not create or confer any right or benefit on any person or party, private or public".

2. European Commission action

On the basis of these new Undertakings the Commission drafted a Decision on the adequate protection of personal data contained in the PNR of air passengers transferred to the United States' Bureau of Customs and Border Protection.

This Decision declares the "adequacy" of the new Undertakings in order to permit the transfer of this data to the US by the airline companies. The legal basis of this Decision is Article 25.6 of Directive 95/46/EC, being this Article an exception to the general principle of Article 25.1 that prohibits the transfer of personal data to countries not assuring an "adequate level of protection".

The Parliament is concerned as to the nature, from a constitutional perspective, of the instrument chosen by the European Commission

At the same time, the Commission has also presented a Proposal for a Council Decision on the conclusion of an Agreement between the European Community and the USA on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.[14]

The legal basis of this proposal is Article 300(2) of the Treaty establishing the European Community. The reasons to adopt such an Agreement are mainly twofold: (1) Direct access by US authorities to PNR databases located in Europe involves the exercise of US sovereignty in EU territory, what needs an explicit consent by EU; (2) Article 7 of the Directive 95/46/EC enunciates restrictively a list of circumstances under which personal data can be processed, and for the time being no legal obligation for air carriers to process PNR data with the purpose of given access and transfer it to the US does exist according to this provision.[15]

So, the proposed Agreement declares that CBP may electronically access the PNR data from air carriers' reservation systems located within the territory of the Member States of the EC in accordance with the Decision and until a satisfactory transmission system is put in place. Furthermore, this instrument would create the obligation for air carriers to process PNR data as required by CBP pursuant to US law. Indeed, this legal obligation is supposed to be created in order to legitimize such a processing under Article 7(c) of Directive 95/46/EC.

3. Reaction of the European Parliament

The European Parliament has reacted to the Commission initiatives expressing its disagreement.[16] Regarding the adequacy Decision (when it still was in its draft status), the Parliament called upon the Commission to withdraw it. As far as the Proposal for an Agreement was concerned, it did not approve of the conclusion in the Agreement, instructing its President to call on the Council not to conclude the Agreement. It also called on the Council to refrain from complicating the Agreement until the Court of Justice delivered its opinion on its compatibility with the Treaty under Article 300(6) of the EC Treaty.

The Agreement is referred to by the majority of the European Parliament as a "light international agreement" because the Parliament was only consulted about it. However, its opinion is not binding. The Parliament is concerned as to the nature, from a constitutional perspective, of the instrument chosen by the European Commission to limit a fundamental right, which may not be the appropriate action.

The (draft) Adequacy Decision, on the other hand, was criticized by the European Parliament for different reasons, eg, for being based on Undertakings that were of purely administrative nature and which content should be improved (e.g., a list of serious crimes in respect of which additional request could be made, the list of authorities and agencies which could access or obtain the PNR data collected by the CBP and the data protection conditions to be respected by these third parties, etc.).

4. The Opinion issued by the Article 29 Personal Data Protection Working Party

The Working Party has issued three Opinions since the negotiations with CBP started. The last one is referred to the new Undertakings (as attached to the draft Commission Decision). The Working Party welcomed the "sunset clause" in Point (46),

under which the undertakings shall apply for a term of three years and a half, and before extending them further discussions should take place. It also welcomed the joint reviews foreseen in Point (43). This audit procedure would be carried out once a year by CBP in conjunction with DHS, and the European Commission, assisted as appropriate by representatives of European law enforcement authorities and/or authorities of the Member States of the European Union.

Nevertheless, the Opinion pointed out several issues that still need to be improved in order to achieve a legitimate framework for the transfer of PNR data. In particular, and among other problems, the Working Party considered that: (1) given the fact that CAPPS II raised particular issues that needs to be clarified, US authorities should refrain from using PNR data for implementing or testing CAPPS II; (2) the purpose limitation principle, even if improved, still presented certain vagueness, specially in what concerns the expression "other serious crimes"; (3) the list of PNR items, which has been reduced from 38 to 34 items, was seen as a very little progress; (4) the processing of sensitive data was also still problematic, specially for what "free text fields" may contain, which deletion should take place in the EU, before the data was transferred; (5) the data retention period, which indeed had been reduced, was considered to remain disproportionate; (6) a precise identification of the other US public bodies entitled to receive the data was required; (7) the access principle presented some concerns, mainly regarding the exceptions that may be opposed to the data subject in order to refuse this right; etc.

At the time when the Working Party issued its Opinion, it did not have access to the draft Agreement. However, it commented that the right to privacy could only be limited following the conditions established by a legislative instrument

5. The Opinion of the Belgian Data Protection Authority

The Belgian DPA has recently issued an Opinion[17] after the complaint submitted by two citizens as a consequence of the transmission of their personal data (PNR and APIS) to the US by US airline companies (Delta Airlines, United Airlines, and Continental Airlines) in different trips that departed from Belgium. The authority analysed the applicable principles, and noted that the purpose limitation principle, the information principle, and the trans-border data flows (TBDF) rules had not been respected by the carriers.

Concerning the purpose limitation principle, it observed that passengers' data were collected and further processed for necessary contractual obligations to carry out the transport of the passenger. The transmission of these data to US authorities went beyond this purpose. Furthermore, the fact that the transmission obligation was foreseen in US legislation did not render it legally binding under EU law. It, thus, could be considered as a legitimate basis for data processing, at least until such obligation was created under EU law.[18]

In respect of the legal obligation to inform the data subject, the Belgian DPA verified that two of the companies did not inform the passengers that their data would be transferred to the US authorities. One of the companies did inform, but this information was considered minimal, taking into account that it neither specified who would be the addressee of it, nor its purpose. Moreover, the means of communication was not explicit enough, insofar the information was integrated into the general conditions terms, which were available upon request or via the Internet.

The last issue analysed was the compliance with TBDF rules. The Opinion made reference to the fact that, so far, the US had not been awarded with an "adequacy" finding Decision issued by the European Commission,[19] not existing, in the analysed case, any other legal basis for making the transfer. This resulted in a transfer made illegally.

C. "Fondo" & "forma" issues

It is evident that there remain many controversial issues to be clarified and ruled out in this intricate and sensitive arena. Some of them deal with the content of the negotiating instruments ("*fondo*") in order to respect not only "adequacy" principles, but also other aspects that need to be further discussed like the problem of EU sovereignty already pointed out in the context of the Echelon case.[20] Others deal with the formalities and legal basis to be used ("*forma*") in order the reach a constitutional respectful arrangement. We will make a brief and not exhaustive reference to some of those issues.

1. "Fondo"

Certain improvement to the classic "adequacy principles" would still be desired, as pointed out

by the Article 29 Data Protection Working Party. They will not be analysed again here, but let us concentrate on other points that should be considered in the very specific case of passengers' data.

Specific concerns that remain regarding the use of PNR and/or APIS data for CAPPS II should be pointed out. Indeed, this system involves specific risks for the protection of personal data which have not been addressed by the Commission Decision. No consideration has been given to the fact that CAPPS II is actually a tool for automated individual decisions, and respect should be given provided to Article 15 of the Directive in the TBDF context. It has to be underlined that it is also one of the principles contained in the Working Document n°12 elaborated by the Article 29 Data Protection Working Party.[21] In this context, even for testing activities, "the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest". Even if the official version of the Decision presents certain few changes (compared to the draft version) in Point (8) of the Undertakings regarding the "purpose" of processing activities in the current context of CAPPS II,[22] respect for Article 15 is still missing.

No consideration has been given to the fact that CAPPS II is actually a tool for automated individual decisions

The reciprocity issue is indeed outside the scope of an "adequacy finding", but from a Public International law perspective is important as a sign of *bona fide* and mutual commitments. However, reciprocity seems not to be sufficiently guaranteed in the new Undertakings. The soft compromise of Point (45) waters down the seriousness of the engagement being assumed. There is no "reciprocity" indeed. A reciprocal engagement would be one where US authorities assume the compromise to impose such legal obligation as the one the EU is seeking to impose within its territory via the adoption of the proposed Agreement.

2. "Forma"

The situation concerning the legal basis is rather complex too. The subject matter involves different levels (or "pillars") of EU law. This creates an insufficiency of the traditional legal basis and instruments used to solve the TBDF problematic. Directive 95/46/EC is a first pillar Directive. Adequacy Decisions have been adopted, so far, mainly thinking about the free movement of data for private bodies' uses (the Safe Harbor could be considered the paradigm of that logic). However, in the passengers' data case, the TBDF solution has to guarantee the airline carriers that the transfer made in this context is legal. Furthermore, the TBDF solution has to guarantee a legitimate transfer to public foreign bodies for the purpose of the fight against terrorism and law enforcement. This exceeds the material scope of the Directive. This is, at EU level, a third pillar matter. Internally speaking, the regulation of such an issue would never be based on Article 95 TEC as is the Directive 95/46/EC.[23]

Nevertheless, the concept of "adequate protection" is, in our opinion, relevant for the third pillar. The Additional Protocol to the Convention n. 108 regarding supervisory authorities and trans-border data flows,[24] which is applicable to the third pillar, explicitly regulates in Article 2.1 that:

*"1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an **adequate** level of protection for the intended data transfer" [emphasis added].*

Other EU instruments of the third pillar also foresee "adequate protection" for TBDF. For instance, Article 18 of the Europol Convention stipulates that:

*"1. Europol may under the conditions laid down in paragraph 4 communicate personal data which it holds to third states and third bodies within the meaning of Article 10(4), where: (…) 2) an **adequate** level of data protection is ensured in that State or that body, (…)"[emphasis added].*

With this being said, even if the Working Document n° 12 has been elaborated in the context of Directive 95/46/EC, the principles described therein, would, in principle, be respected also in a third pillar framework. Perhaps, what needs to be better defined is the legal basis for the "Adequacy" finding referred in this paper.

Apart from that, there are other formal requirements that have to be respected. Article 8.2 of the European Convention for the protection of Human Rights and Fundamental Freedoms requires that limitations to the right to privacy by public authorities must be in accordance with the law and necessary in a democratic society. In the commented case, there remain doubts about the pertinence of an adequacy Decision based on unilateral Undertakings of the CBP and even of

the proposed Agreement, from a constitutional perspective. Strasbourg case law[25] explains that Article 8.2 requires the adoption of a "legislative text" in the formal sense, meaning that the intervention of the Legislative power ought to be effective in the drafting and adoption process.

D. Concluding remarks

In fact, due to the present state of the passengers' data debate, it is not yet possible to give a final conclusion. This paper remains open to upcoming actions to come at the EU level, and also, potentially, at the national level as the Belgian case shows. Word has been given to the European Court of Justice, which is welcomed due to the sensitivity of the issues at stake.

It is regrettable that personal data have been transferred in violation of the law and without any legal framework to regulate that anomalous situation. Personal data transferred seems to be a "no man's land" story. However, "urgency" could be also risky if a proper balance between conflicting legitimate interests is not properly respected in decision-making processes.

It would be interesting to see if the third pillar implications are finally addressed. The airline passengers' case could be quite paradigmatic in relation to the limits of the application of Directive 95/46/EC to deal with TBDF made beyond the first pillar of EU law.

Verónica Pérez Asinari Lawyer, Researcher at the CRID and **Yves Poullet**, Dean of the Faculty of Law, Director of the CRID. Professor at the Universities of Namur and Liege *Centre de Recherches Informatique et Droit* (CRID), University of Namur, Belgium

http://www.crid.be

FOOTNOTES

1 M.V. Perez Asinari and Y. Poullet "The airline passenger data disclosure case and the EU-US debate", [2004] 20 CLSR 98-116.

2 Mainly the Aviation and Transportation Security Act (ATSA), Public Law 107-71, 107th Congress.

3 Commission Decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name record of air passengers transferred to the United States' Bureau of Customs and Border Protection, C(2004) 1914, available at: http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/pnr/c-2004-1914/c-2004-1914_en.pdf.

4 EU Institutions press releases "Commission secures guarantees for protecting personal data of transatlantic air passengers", 17/05/2004, available at: http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/04/650&format=HTML&aged=0&language=EN&guiLanguage=en

5 "According to the case law of the Court, the European Parliament's request for an opinion will be devoid of purpose if the agreement is concluded by the Council. However, the Parliament would then have the option of exercising its right under Article 230 of the EC Treaty to seek the annulment of the international agreement or of the adequacy finding or both", EU Institutions press releases "Commission secures guarantees for protecting personal data of transatlantic air passengers".

6 Convention for the Protection of Human Rights and Fundamental Freedoms ETS no.: 005, Rome 4/11/50. Available at: http://conventions.coe.int/treaty/en/WhatYouWant.asp?NT=005

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEC L 281 23/11/1995, p. 31 – 50, hereinafter quoted: "the Directive".

8 Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration, available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78-pnrf-annex_en.pdf.

9 See Article 29 Data Protection Working Party, Opinion *6/2002 on transmission of Passenger manifest Information and other data from Airlines to the United States*, 24 October 2002, WP 66. Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data*, 13 June 2003, WP 78.

10 The European Commission drafted a complementary "Agreement" based in Article 300 (2) TEC. See also our analysis of the legal basis: M.V. Perez Asinari and Y. Poullet "The airline passenger data…", op. cit., p. 103 and ss.

11 The new Undertakings are annexed to the Commission Decision on the adequate protection of personal data contained in the PNR of air passengers transferred to the United States'.

12 The principles that should be respected are expressed in Article 29 Working Party, *Working Document Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 24 1998, WP 12.

13 For a description of CAPPS II system see M.V. Perez Asinari and Y. Poullet "The airline passenger data…", op. cit., p. 100. It is basically a system to conduct risk assessments for passenger and aviation security. It presents many privacy and personal data protection concerns.

14 Brussels, 17.03.2004, COM(2004)190 final, 2004/00645CNS), available at : http://europa.eu.int/eur-lex/en/com/pdf/2004/com2004_0190en01.pdf.

15 See: European Parliament, Report on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (COM(2004) 190 – C5-0162/2004 – 2004/0064(CNS)) Committee on Citizens' Freedoms and Rights, Justice and Home Affairs Rapporteur: Johanna L.A. Boogerd-Quaak, 7 April 2004.

16 European Parliament, Report on the proposal for a Council decision on the conclusion of an Agreement between the European Community and the United States

of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (COM(2004) 190 – C5-0162/2004 – 2004/0064(CNS)) Committee on Citizens' Freedoms and Rights, Justice and Home Affairs Rapporteur: Johanna L.A. Boogerd-Quaak, 7 April 2004. European Parliament Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (2004/2011(INI)).

17 Avis n° 48/2003/ANO du 18 décembre 2003. Objet : Plaintes relatives à la transmission de données à caractère personnel par certains compagnies aériennes vers les Etats-Unis.

18 In such a hypothetical case, the processing would be legitimated under article 7(c) of the Directive. See already the reasoning held on that point by the European Commission.

19 See in our previous paper the explanation as of why the Safe Harbour Decision is not applicable in this realm. M.V. Perez Asinari and Y. Poullet "The airline passenger data…", op. cit., p. 106. There we make reference to European companies, which are not under the jurisdiction of the Federal Trade Commission or the Department of Transportation. However, even if US companies were to be analysed, the Safe Harbour Principles would not be applicable anyway, since the matter under study deals with "law enforcement" and not with "consumer protection", what is actually the structure under which the Safe Harbour is built.

20 About this delicate debate and the need for a new approach of the sovereignty principle, see Y. Poullet, "Le droit et le devoir de l'Union Européenne et des Etats Membres de veiller au respect de la protection des données dans le commerce mondial", in *The Spanish Constitution in the European Constitutional Context*, F. Fernández Segado (ed.), Dykinson, Madrid, 2003, 1764 and ff.

21 Article 29 Data Protection Working Party, Working Document *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998, WP 12.

22 "(…)The purpose of the processing is strictly limited to testing the CAPPS II system and interfaces, and, except in emergency situations involving the positive identification of a known terrorist or individual with established connections to terrorism, is not to have any operational consequences. (…)".

23 Former Article 100(A) TEC.

24 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8.XI.2001, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm.

25 For instance, European Court of Human Rights, Case of P.G. and J.H. v. the United Kingdom, Application no. 44787/98, Judgment, Strasbourg, 25 September 2001.